IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

DAVID BERNSTEIN (a Montgomery County, Maryland Resident), RICHARD DAVIS, DANIEL MEYERSON, JOEL NICE, and SERAPHIN NICHOLSON, individually and on behalf of all others similarly situated, **Plaintiffs,** **v.** **MARRIOTT INTERNATIONAL, INC.,** **10400 Fernwood Rd.** **Bethesda, Maryland 20817** **(a Montgomery County, Maryland Resident)** **Defendant.**	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs David Bernstein, Richard Davis, Daniel Meyerson, Joel Nice, and Seraphin Nicholson ("Plaintiffs"), individually and on behalf of all other similarly situated individuals, allege upon personal knowledge of the facts respectively pertaining to them and upon information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant Marriott International, Inc. ("Defendant" or "Marriott").

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Marriott for its failure to exercise reasonable care in securing and safeguarding its guests' sensitive personal information ("SPI"), including its guests' names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, date of birth, gender, arrival and

departure information, reservation date, communication preferences and payment card information.

2. Marriott became the largest hotel chain in the world on September 23, 2016 when it acquired Starwood Hotels and Resorts Worldwide, LLC ("Starwood"). As part of its acquisition of Starwood, Marriott took control of Starwood's reservation system and the Starwood Preferred Guest loyalty program.

3. The Starwood Preferred Guest loyalty program collected the SPI of Starwood's guests. Marriott maintained the Starwood Preferred Guest loyalty program separately until August 18, 2018, when it was combined with Marriott's existing customer loyalty program (Marriott Rewards). Thereafter, Marriott continued to maintain the SPI collected through the Starwood Preferred Guest loyalty program.

4. On November 30, 2018, Marriott announced that it learned on September 8, 2018, of an unauthorized access to its Starwood guest reservation database for reservations extending until September 10, 2018, but going back at least as early as 2014.[1] Marriott announced that the breach affected at least 500 million people, and that for 327 million people, information containing the "name, mailing address, phone number, email address, passport number, Starwood Preferred Guest loyalty program account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences" was taken.[2]

5. Marriott disclosed that even though payment card information for affected individuals, including payment card numbers and expiration dates, was encrypted, it could not

[1] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/, last accessed November 30, 2018.
[2] *Id.*

rule out the possibility that the means to decrypt this information was not also taken.[3]

6. Further, Bloomberg reported that the unknown thieves may be capable of stealing the Starwood loyalty points in accounts of those whose information was stolen as part of the security breach.[4]

7. Marriott also disclosed that the information in Marriott's Starwood database was accessed and copied, and that unknown parties "took steps towards removing it."[5]

8. Marriott's security failures enabled the data thieves to seal Plaintiffs' and the Class members' SPI. These failures put Plaintiffs' and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members from time spent and the loss of productivity in taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the theft of their SPI, and the resulting stress, nuisance and annoyance.

9. Marriott's data security breach was caused and enabled by Marriott's knowing violation of its obligation to abide by best practices and industry standards. Marriott failed to abide by security standards and allowed its guests' SPI to be compromised by failing to take measures that could have prevented or mitigated the security breach that occurred.

10. Plaintiffs and members of the Class must now guard against both the unauthorized use of their payment card information and against identity theft, including but not limited to the cloning of fraudulent passports. Plaintiffs must also guard against the unauthorized use of their Starwood Preferred Guest loyalty reward points by the data thieves or other fraudsters.

---

[3] *Id.*

[4] *See* https://www.bloomberg.com/news/articles/2018-11-30/all-those-starwood-points-you-racked-up-at-risk-in-marriott-hack, last accessed November 30, 2018.

[5] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/, last accessed November 30, 2018.

PARTIES

11. Plaintiff David Bernstein is a resident of Maryland (Montgomery County). He is a member of the Starwood Preferred Guest loyalty program prior to its merger with the Marriott Rewards program in August 2018 and had his SPI on file with Marriott as part of his membership in the program. His information was accessed as part of the unauthorized access detailed in this complaint.

12. Plaintiff Richard Davis is a resident of Illinois. He is a member of the Starwood Preferred Guest loyalty program prior to its merger with the Marriott Rewards program in August 2018 and had his SPI on file with Marriott as part of his membership in the program. His information was accessed as part of the unauthorized access detailed in this complaint.

13. Plaintiff Daniel Meyerson is a resident of the District of Columbia. He is a member of the Starwood Preferred Guest loyalty program prior to its merger with the Marriott Rewards program in August 2018 and had his SPI on file with Marriott as part of his membership in the program. His information was accessed as part of the unauthorized access detailed in this complaint.

14. Plaintiff Joel Nice is a resident of Massachusetts. He is a member of the Starwood Preferred Guest loyalty program prior to its merger with the Marriott Rewards program in August 2018 and had his SPI on file with Marriott as part of his membership in the program. His information was accessed as part of the unauthorized access detailed in this complaint.

15. Plaintiff Seraphin Nicholson is a resident of Connecticut. She is a member of the Starwood Preferred Guest loyalty program prior to its merger with the Marriott Rewards program in August 2018 and had her SPI on file with Marriott as part of her membership in the

program. Her information was accessed as part of the unauthorized access detailed in this complaint.

16. Defendant Marriott International, Inc. is a Delaware corporation with its principal place of business at 10400 Fernwood Rd, Bethesda MD 20817 (Montgomery County).

JURISDICTION AND VENUE

17. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, and there are 100 or more members of the Class.

18. This Court has personal jurisdiction over Marriott because it has its principal place of business in Maryland and regularly conducts business in Maryland.

19. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because Defendant has its principal place of business in this district and regularly conducts business in this district. Marriott is therefore subject to general jurisdiction in this district.

FACTUAL ALLEGATIONS

Marriott's Data Collection Practices

20. As stated above, Marriott is the world's largest hotel chain. Prior to its acquisition of Starwood, Starwood had more than 1,200 hotels worldwide operating under a Starwood brand.[6]

21. Customers reserving hotels within the Starwood system were encouraged to set up a Starwood Preferred Guest customer loyalty account. These accounts collected, among other information, full names and addresses, payment card numbers, payment card expiration dates,

[6] *See* https://www.starwoodhotels.com/Media/PDF/Corporate/GC_Report_2014.pdf, p. 5, last accessed November 30, 2018.

and passport numbers. This information was retained in Starwood's – and later Marriott's – system for convenience in reserving future hotel rooms.

The Data Breach

22. At some time before September 8, 2018, and possibly going back to 2014 (if not prior to that), unauthorized users accessed, copied, and "took steps to toward[] removing" what appears to be the entirety of the Starwood guest reservation database.[7] Marriott disclosed that this included information for up to 500 million users, including more detailed information (as described above) for 327 million users.

23. Marriott discovered the unauthorized access on September 8, 2018, but did not notify the public of this information until almost three months later on November 30, 2018.[8]

24. Marriott disclosed that 327-million-person subset whose more detailed SPI was stolen included payment card numbers and expiration dates, purportedly in encrypted form. However, Marriott also stated that both of the components needed to decrypt the payment card information may have also been taken.[9]

25. According to Marriott's public statements, the only SPI that was encrypted was its guests' payment card information. The passport numbers that were stolen were therefore *not* encrypted.[10]

26. The fact that Marriott believes its encryption key may also have been stolen indicates that Marriott did not store its encryption key in a cryptographic vault, as is required

[7] *See* http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/, last accessed November 30, 2018.
[8] *Id.*
[9] *Id.*
[10] *Id.*

under standard data security best practices.[11] Instead, Marriott likely retained its encryption key in the same location as the data it was meant to encrypt, rendering the encryption much less valuable and more easily able to be compromised.

27. Noted cybersecurity expert Brian Krebs observed that the hospitality industry, in particular, has seen repeated public failures in data security.[12] The Intercontinental Hotels Group, Hyatt, and Kimpton Hotels have all seen high-profile breaches in the last three years. Accordingly, Marriott was aware of the importance of maintaining proper control over the security of its guests' SPI and of the likelihood of thieves trying to steal it.

28. Krebs further noted that "even the web site used to disclose this breach can't be bothered to use [a secure website]. These may seem like little things, but they are very public things. Makes you wonder what it looks like on the inside."[13]

Defendant Did Not Properly Safeguard its Guests' SPI

29. Defendant's treatment of the SPI entrusted to it by the members of the Class fell far short of its obligations. Defendant failed to ensure that access to its data systems was reasonably protected.

30. Marriot is subject to federal security standards and recommendations intended to reduce data breaches and the resulting harm to consumers. The Federal Trade Commission ("FTC") issues guidance to businesses, emphasizing reasonable data security practices. The

[11] *See* https://www.owasp.org/index.php/Key_Management_Cheat_Sheet#Storage, last accessed November 30, 2018.
[12] *See* https://twitter.com/briankrebs/status/1068505042150400001, last accessed November 30, 2018.
[13] *See* https://twitter.com/briankrebs/status/1068505635556376576, last accessed November 30, 2018.

current FTC guidelines, in place since 2016,[14] note that businesses should:

- protect the personal customer information that they keep;
- properly dispose of personal information that is no longer needed;
- encrypt information stored on computer networks; understand their network's vulnerabilities; and
- implement policies to correct security problems.

31. The guidelines also recommend that businesses:

- use an intrusion detection system to expose a breach as soon as it occurs;
- monitor all incoming traffic for activity indicating someone is attempting to hack the system;
- watch for large amounts of data being transmitted from the system; and
- have a response plan ready in the event of a breach.

32. Finally, the FTC recommends companies:

- not maintain cardholder information longer than is needed for authorization of a transaction;
- limit access to sensitive data;
- require complex passwords to be used on networks;
- use industry-tested methods for security;
- monitor for suspicious activity on the network; and
- verify that third-party service providers have implemented reasonable security measures.[15]

[14] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, last accessed November 30, 2018.
[15] *See* Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf, last accessed November 30, 2018.

33. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data. It treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

34. Marriott was at all times fully aware of its obligation to protect its guests' SPI. Defendant was also aware of the consequences if it did not adequately protect that information, both to itself (in exposure to the FTC and civil litigation) and to its guests (in the form of the costs associated with data breach and exposure to identity theft).

35. As a result of Defendants' failure to adhere to industry and government standards for the security of its guests' SPI, the SPI of 500 million of Defendant's guests, including Plaintiffs, was compromised over at least four years if not longer.

The Monetary Value of Privacy Protections and SPI

36. The very targeting of the Class members' SPI demonstrates its monetary value. Privacy breaches are no longer the province predominantly of lone bad actors or thrill seekers, but now constitute an international fraud industry.

37. As early as 2001, then-FTC Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[16]

[16] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at

38. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[17] More recently, former Commissioner Pamela Jones Harbour underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[18]

39. Because of the value that consumers place on their SPI, many companies now offer consumers an opportunity to sell this information.[19] Consumers thereby gain more control over the information they share and who receives that information, and, by making the transaction transparent, consumers profit from their own SPI.

40. Accordingly, any company that transacts business with consumers and then compromises the privacy of consumers' SPI has thus deprived consumers of the full monetary value of their transaction with the company.

The Effect of the Data Breach on Plaintiffs and the Class

41. Plaintiffs and the Class now face a real and immediate risk of identity theft and fraudulent payment card charges resulting from Defendant's actions, including its decision to

---

https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf, last accessed November 30, 2018.

[17] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html, last accessed November 30, 2018.

[18] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf, last accessed November 30, 2018.

[19] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html, last accessed November 30, 2018.

delay public notification of the breach.The processes of discovering and dealing with the repercussions of identity theft and fraudulent payments are time consuming and difficult. The Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[20]

42. The victims here, Plaintiffs and the Class (defined below), are no different, as they are faced with an arduous path to secure their SPI in response to Defendant's negligence.

43. Best practices require Plaintiffs and the Class to take the following labor intensive and time consuming steps to attempt to prevent further misuse of their SPI:

- Review and monitor credit card statements for any unusual or unknown charges.
- Contact their financial institution to determine if there is any suspicious activity on their accounts.
- Change their account information.
- Place a fraud alert on their credit bureau reports.
- Place a security freeze on their credit bureau reports.
- Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

44. Even then, there is no guarantee that any such measures will be successful. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when SPI is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on

[20] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics Dec. 2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf, last accessed November 30, 2018.

> the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

45. There is a very strong probability that those impacted by Defendant's failure to secure the SPI could be at risk of fraud and identity theft for extended periods of time.

46. Further, passport numbers are useful to people who seek to steal identities and create fraudulent passports.[22] Passport numbers also generally only change every ten years, when a passport is updated, and so can be valuable to hackers and thieves for a longer period of time.

47. Moreover, Plaintiffs are at risk for having their Starwood Preferred Guest loyalty reward points stolen by the data thieves. A data thief may easily redeem reward points belonging to a guest whose SPI was stolen, exchanging reward points for airline miles, gift cards, or physical goods from the program's shopping portal. A data thief may also redeem reward points for hotel stays or flights, which can be cancelled in exchange for a gift card. Unlike issuers of credit cards, Defendant is not legally obligated to make defrauded guests whole for their stolen reward points.[23]

48. As a result of Defendant's negligent security practices, Plaintiffs and the Class have been exposed to fraud, have directly incurred damages, and face a heightened and imminent risk of fraud and identity theft. Plaintiffs and the Class must now and in the future closely monitor their financial accounts to guard against identity theft and fraudulent charges. Further,

---

[21] U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf, last accessed November 30, 2018.

[22] *See* https://blog.credit.com/2014/05/numbers-identity-thieves-want-83924/, last accessed November 30, 2018.

[23] *See* https://www.bloomberg.com/news/articles/2018-11-30/all-those-starwood-points-you-racked-up-at-risk-in-marriott-hack, last accessed November 30, 2018.

Plaintiffs and the Class must also monitor against possible identity theft when travelling. Plaintiffs and the Class may be faced with fraudulent debt or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services and obtaining credit reports, credit freezes, and other protective measures to deter, detect, and mitigate the risk of identity theft and fraud, as well as obtaining new passports or other travel documents. Some have already incurred costs in doing so.

CLASS ACTION ALLEGATIONS

49. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), seeking damages and equitable relief on behalf of the following Class:

> All persons whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.

50. Further, Plaintiff David Bernstein brings this action on behalf of himself and as a class action under Fed. R. Civ. P. 23, seeking damages on behalf of the following Maryland Subclass:

> All Maryland residents whose SPI was accessed and/or compromised by unauthorized individuals as part of the data breach at issue in this litigation.

51. Excluded from the Class and Subclass are Defendant; any parent, affiliate, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any of Defendant's officers or directors; or any successor or assign of Defendant. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

52. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The Class is so numerous that joinder of all members is impracticable. While Plaintiff does not know the exact

number of the members of the Class, Plaintiff believes it contains hundreds of millions of members with tens of thousands in Maryland.

53. **Commonality and Predominance – Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and Subclass. Such questions of law and fact common to the Class include, but are not limited to:

(a) Whether Defendant engaged in the wrongful conduct alleged herein;

(b) Whether Defendant owed a duty to Plaintiffs and members of the Class and Subclass to adequately protect their SPI;

(c) Whether Defendant breached its duty to adequately protect the SPI of Plaintiffs and members of the Class and Subclass;

(d) Whether Defendant should have known that its data systems and processes were vulnerable to attack and taken sufficient steps to prevent such attack;

(e) Whether Defendant's conduct, including its failure to act, was the proximate cause of, or resulted in, the breach of its database containing SPI;

(f) Whether Plaintiffs and members of the Class and Subclass suffered legally cognizable damages as a result of Defendant's conduct and are entitled to recover damages;

(g) Whether Plaintiffs and members of the Class and Subclass are entitled to equitable relief.

54. The questions of law and fact common to the members of the Class and Subclass predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

55. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the members of the Class and Subclass, and Plaintiffs will fairly and

adequately protect the interests of the Class and Subclass. Plaintiffs and all members of the Class and Subclass are similarly affected by Defendant's wrongful conduct in that their information was exposed to unauthorized users in violation of federal, state and common law.

56. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class and Subclass. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Class and Subclass. Plaintiffs are represented by counsel who are competent and experienced in the prosecution of security breach and class action litigation.

57. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class and Subclass would continue to suffer the harm described herein, for which they have no remedy. Even if separate actions could be brought by individual guests, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, and created a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Marriott.

58. **Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Marriott has acted and/or refused to act on grounds that apply generally to the Class and Subclass, making injunctive and/or declaratory relief appropriate with respect to the Class and Subclass under Federaul Rule Civil Procedure 23(b)(2).

59. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** Class action treatment is a superior method for the fair and efficient adjudication of the controversy, in that, among

other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Plaintiffs and the Class)

60. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

61. Defendant solicited and took possession of the SPI of Plaintiffs and the Class and had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Defendant also had a duty to timely notify Plaintiffs and the Class that their SPI had been or may have been stolen. Defendant further had a duty to destroy the SPI of Plaintiffs and members of the Class within an appropriate amount of time after it was no longer required by Marriott in order to mitigate the risk of such non-essential SPI being compromised in a data breach.

62. Defendant's duties arose from its relationship to Plaintiffs and Class members and from industry custom and practice.

63. Defendant, through its actions and/or failures to act, unlawfully breached duties to Plaintiffs and Class members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the SPI entrusted to it.

64. Defendant's failure to exercise reasonable care in safeguarding SPI by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiffs' and Class members' SPI being accessed and stolen through the data breach.

65. As a result of Defendant's breach of duties, Plaintiffs and members of the Class have been injured and have suffered damages, including having credit card accounts fraudulently applied for in their names, lowered credit scores, and being required to expend time and money to prospectively and/or remedially address the harm created by the data breach.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

66. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

67. Plaintiffs and members of the Class reasonably believed that in providing SPI to Defendant, in exchange for the ability to reserve hotel rooms and guest services and to accrue Starwood loyalty program points, their SPI would be protected with adequate security measures. This transaction amounts to an implied agreement with Defendant that the SPI provided will be safeguarded as one of the obligations of Marriott.

68. Defendant solicited the SPI in exchange for allowing Plaintiffs and members of the Class to enroll in the Starwood Preferred Guest loyalty program and reserve Starwood rooms. Plaintiffs and the Class accepted Defendant's offer and provided their SPI as well as reserving rooms in the Starwood reservations system.

69. This implied agreement was mutually agreed to between Plaintiffs and members of the Class on one hand, and Defendant on the other.

70. Plaintiffs and members of the Class would not have provided Defendant with their SPI in the absence of the implied agreement that Defendant would protect such information.

71. Plaintiffs and members of the Class fully performed their obligations under their implied agreements with Defendant.

72. Defendant breached its implied agreement with Plaintiffs and members of the Class to protect their SPI by (1) failing to implement security measures designed to prevent this attack; (2) failing to employ sufficient security protocols to detect the unauthorized network activity; (3) failing to maintain basic security measures such as reasonably segregating its encryption keys so that if data were stolen it would be unreadable or unusable; and (4) failing to provide timely and accurate notice to Plaintiffs and members of the Class that their SPI was accessed and compromised through the data breach. Defendant's failure to properly secure the SPI and notify Plaintiffs and members of the Class about the breach is the direct and proximate cause of the damages suffered by Plaintiffs and the Class.

73. Plaintiffs and members of the Class have been damaged by Defendant's breach of its implied agreement because, *inter alia*, their SPI has been compromised and are at increased risk of future identity theft. Plaintiffs and members of the Class have also been deprived of the value of their SPI and have lost money and property as a result of Defendant's unlawful and unfair conduct.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

74. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

75. Plaintiffs and members of the Class enriched Defendant by entrusting their SPI to Defendant.

76. Defendant appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein.

FOURTH CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

77. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

78. Section 5 of the FTCA prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect its guests' SPI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

79. Marriott's violation of Section 5 of the FTCA constitutes negligence per se.

80. Plaintiffs and Class members are within the class of persons that the FTCA was intended to protect.

81. The harm that occurred as a result of the theft of SPI is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

82. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class will suffer injuries, including but not limited to damages from lost time and effort to mitigate the actual and potential impact of the theft of SPI including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial

institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. Guests whose payment card information was stolen may also become unable to use their payment cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the theft of their SPI; and false or fraudulent charges stemming from the theft of their SPI, including but not limited to late fees charged and forgone cash back rewards.

FIFTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

83. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

84. Plaintiffs and members of the Class entered into an implied contract that required Defendant to provide adequate security for the personal information it collected from Plaintiffs and Class members' participation in the Starwood Preferred Guest rewards program.

85. Defendant owes duties of care to Plaintiffs and the members of the Class which would require it to adequately secure personal information.

86. Defendant still possesses personal information regarding Plaintiffs and the Class members.

87. Marriott has provided no details about what, if any, fixes it has implemented to safeguard the SPI of Plaintiffs and the Class.

88. Accordingly, Marriott still has not satisfied its contractual obligations and legal duties to Plaintiffs. In fact, now that Marriott's lax approach towards information security has

become public, the personal information in Defendant's possession is more vulnerable than previously.

89. Actual harm has arisen in the wake of the security breach regarding Marriott's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their personal information and Defendant's failure to address the security failings that lead to such exposure.

90. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

91. Plaintiffs, therefore, seek a declaration that (1) Marriott's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) to comply with its contractual obligations and duties of care, Marriott must implement and maintain reasonable security measures, including, but not limited to:

a. ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Marriott's systems on a periodic basis, and ordering Marriott to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Marriott audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Marriott segment customer data by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. ordering that Marriott purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. ordering that Marriott conduct regular database scanning and security checks;

g. ordering that Marriott routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Marriott to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Marriott customers must take to protect themselves.

SIXTH CLAIM FOR RELIEF
Violation of Maryland Consumer Protection Act
(On Behalf of Plaintiff David Bernstein and the Maryland Subclass)

92. Plaintiff David Bernstein incorporates all prior paragraphs as though fully set forth herein.

93. Plaintiff David Bernstein and the Maryland Subclass are consumers within the meanings of Md. Commercial Law Code Ann. § 13-101(c) and customers within the meaning of Md. Commercial Law Code Ann. § 14-3502(a).

94. Defendant failed to implement and/or maintain reasonable security procedures or protect the SPI of Plaintiffs and the Maryland Subclass as required by Md. Commercial Law Code Ann. § 14-3503(a).

95. Defendant's failure led to unauthorized access and/or use of Plaintiff David Bernstein and the Maryland Subclass's SPI.

96. Defendant's failure is a "breach of the security of a system" as defined in Md. Commercial Law Code Ann. § 14-3504(a).

97. Defendant is liable to Plaintiff David Bernstein and the Maryland Subclass for damages, including reasonable attorney's fees, as set out in Md. Commercial Law Code Ann. § 14-3508(1) and Md. Commercial Law Code Ann. § 13-408(a)-(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully seek from the Court the following relief:

a. Certification of the Class and Maryland Subclass as requested herein;

b. Appointment of Plaintiffs as Class and Subclass representatives and their undersigned counsel as Class counsel;

c. Award Plaintiffs and members of the proposed Class and Subclass damages;

d. Award Plaintiffs and members of the proposed Class and Subclass equitable, injunctive and declaratory relief, including the enjoining of Defendant's insufficient data protection practices at issue herein and Defendant's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Defendant's acts and practices with respect to the safekeeping of SPI are negligent;

f. Award Plaintiffs and members of the proposed Class and Subclass pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and members of the proposed Class and Subclass reasonable attorneys fees and costs of suit, including expert witness fees; and

h. Award Plaintiffs and members of the proposed Class and Subclass any further relief the Court deems proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: December 3, 2018

/s/ Mila F. Bartos
Mila F. Bartos (Bar # 13550)
FINKELSTEIN THOMPSON LLP
3201 New Mexico, NW
Suite 395
Washington, D.C. 20016
Telephone: 202/337-8000
Facsimile: 202/337-8090
mbartos@finkelsteinthompson.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Jeffrey Smith
Matthew M. Guiney
Daniel Tepper
Gloria Kui Melwani
(*pro hac vice forthcoming*)
270 Madison Avenue
New York, New York 10016
Telephone: 212/545-4600
Facsimile: 212/545-4653
smith@whafh.com
guiney@whafh.com
tepper@whafh.com
melwani@whafh.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl Malmstrom
(*pro hac vice forthcoming*)
111 W. Jackson St., Suite 1700
Chicago, IL 60604

Telephone: 312/984-0000
Facsimile: 312/212-4401
malmstrom@whafh.com

Attorneys for Plaintiffs and the Putative Class